REMARKS

In the aforementioned final Office Action, claims 1-38 were examined and rejected. In view of the following remarks, Applicant respectfully requests reconsideration of the application.

Response to Arguments

In paragraphs 1-4 (pages 2-3) of the final Office Action, the Examiner asserts that the Applicant's arguments are not persuasive because the elements Applicant maintains are not found in the cited references are present. Applicant disagrees and provides further arguments below.

Rejection Under 35 U.S.C. §102

In paragraph 2 and on pages 3-4, claims 1-37 were rejected under 35 U.S.C. §102 as being anticipated by *Ginter* (USPN 6,253,193). Applicant respectfully traverses.

Ginter does not contemplate having encrypted access information in the header

Claim 1 recites in part, "a client module configured to generate ***a header comprising encrypted security information as to who and how*** a file including the electronic ***data can be accessed***." In embodiments of the present invention, the security information comprise access rules which determine or regulate who and/or how the document can be accessed and a file key to access the document. "The security information is then encrypted by a cipher with a user key associated with an authorized user to produce encrypted security information." See [0052]. "[T]o access a secured document, a user needs a user key or keys to decrypt the encrypted security information or header first." See [0059].

In contrast, *Ginter* does not contemplate the use of an encrypted header comprising security information which contemplates who and how a file can be accessed. Col. 128, ln. 25-40 of *Ginter* refers to "a logical object structure which includes a 'private body' containing or referencing a set of methods (i.e., programs or procedures) that control use and distribution of the object." This ***private body is located outside of both a "public (or unencrypted) header*** 802 that identifies the object and may also identify one or more owners of rights in the object..." ***or a "private (or encrypted) header*** 804" (Col. 128, ln. 10-20).

While the private header may include a part or all of the information in the public header and may include additional data for validating and identifying the object 300, the validation of the object is not the same as validation of a user (i.e., individual trying to access the data). In fact, *Ginter* distinguishes the two by reciting "data for validating and identifying the object 300 when a user attempts to register as a user of the object" (col. 128, ln. 17-19).

Furthermore, "information identifying one or more rights owners and/or distributors of the object" does not refer to the user attempting to access the object. Instead, rights owners and distributors are exactly as they are termed – "owners of rights in the object and... distributors of the object" (col. 128, ln. 14-15). *Ginter* distinguishes right owners and distributors from a user in this paragraph (col. 128, ln. 11-24) by explicitly using the three terms to describe the different types of individuals that are associated with the object – "right owners," "distributors," and "a user."

Finally, the reference to "any of ***said*** additional validating and identifying data" (col. 128, ln. 23-24), refers back to "the additional data for validating and identifying the object 300" (col. 128, ln. 17-18). As previously discussed, the validation of the object 300 is not the same as validation of a user.

Further, Col. 32, ln. 34-39 of *Ginter* merely discusses how "new control information might specify, for example, who may use at least a portion of the new object, and/or how said at least a portion of said extracted content may be used." This cited portion, however, only refers to how "the extractor of content may add new control methods and/or modify control parameter data, such as VDE (Virtual Distribution Environment) application compliant methods, to the extent allowed by the content's in-place control information." (Col. 32, ln. 30-34). There is no discussion or suggestion that this control information is encrypted or placed into an encrypted header of a secured file in order to control access to the secured file.

As such, *Ginter* does not contemplate "a client module configured to generate a header comprising encrypted security information as to who and how a file including the electronic data can be accessed" as contemplated in claim 1. Therefore claim 1 is not anticipated by *Ginter*. Additionally, because claims 2-16 depend either directly or indirectly from claim 1, these claims are not anticipated for the same reasons as claim 1.

In paragraph 4, claim 33 was rejected for the same reasons as that of claim 1. Claim 33 recites in part "integrating a header comprising encrypted security information with the encrypted data portion to generate a secured file, wherein ***the encrypted security information comprises the file key and access rules*** to control the restricted access to the electronic data." As discussed above with respect to claim 1, the security information, and thus the header, is encrypted by a cipher with a user key associated with an authorized user to produce encrypted security information including access rules. Because *Ginter* does not contemplate having a header comprising encrypted security information including access rules, claim 33 is not anticipated by *Ginter*. Additionally, claims 34-37, which depend either directly or indirectly from claim 33, are not anticipated for the same reasons as that of claim 33.

Ginter does not contemplate a header having access rules

In paragraph 3 and pages 4-5, the Examiner maintained the rejection to claims 17. Independent claim 17 recites in part "a client module configured to generate a header including an encrypted file key and a rule block having N encrypted segments, each of the N encrypted segments including a set of access rules facilitating the restricted access to a file including the electronic data." As discussed above with respect to claim 1, *Ginter* does not discuss or suggest having encrypted security information within the header, whereby the encrypted security information comprises access rules.

The cited portion of *Ginter* referred to by the Examiner is related to ***permission records which "may include key block(s) 810,*** which may store decryption keys for accessing the content of the encrypted content stored within the object 300." (Col. 128 ln. 45-48). The ***permission records, however, are not encrypted security information in a header*** (i.e., the private header in *Ginter*) of a secured file as contemplated by claim 17 (see Figure 17).

The remainder of col. 128 of *Ginter* refers to the content portion of the object which may be divided into data block. These "[d]ata blocks may contain any sort of electronic information, such as, "content, including computer program, images, sound, VDE administrative information, etc." (Col. 128, ln. 49-53) This content portion is essentially equivalent to the document portion of the present invention. That is the data blocks of this cited portion are part of the document not the "N encrypted segments" of the header as claimed in claim 17.

The encryption of the permission record and key blocks as contemplated in col. 129, ln. 18-20, does not cure the defect of col. 128. That is the mere encryption of the permission record and key blocks still does not result in a "header including an encrypted file key and a rule block having N encrypted segments, each of the N encrypted segments including a set of access rules facilitating the restricted access to a file including the electronic data."

Therefore, claim 17 is not anticipated by *Ginter*. Furthermore, because claims 18-32 depend either directly or indirectly from claim 17, these claims are not anticipated for the same reasons as that of claim 17.

Rejection Under 35 U.S.C. §103

On pages 10-11 of the final Office Action, claim 38 was rejected as being unpatentable over *Ginter* in view of *Folmsbee* (USPN 6,308,256). As discussed above with reference to both claims 1 and 33, *Ginter* does not contemplate having a header comprising the encrypted security information which includes the access information. The addition of *Folmsbee* does not cure the deficiencies of *Ginter*. As such, claim 38, which depends from claim 33, is not obvious over *Ginter* in view of *Folmsbee*.

Conclusion

Based on the above remarks, Applicant believes that the rejections in the Office Action of November 29, 2005 are fully overcome, and that the application is in condition for allowance. If the Examiner has questions regarding the case, the Examiner is invited to contact Applicant's undersigned representative at the number given below.

Respectfully submitted,

Denis Jacques Paul Garcia

Date: May 30, 2006

By: Susan Yee
Susan Yee, Reg. No. 41,388
Carr & Ferrell LLP
2200 Geng Road
Palo Alto, CA 94303
Phone: (650) 812-3400
Fax: (650) 812-3444